packets in an authentication flow involving the end-node and wherein the end-node is authorized based at least in part on the verification of the user information to transmit and receive through the edge node packets in data flows involving the end-node and other nodes in the institutional LAN.

45. An edge node for authorizing an end-node to an institutional LAN, the edge node comprising:

an interface for receiving user information from the end-node via a LAN link for verification,

wherein prior to verification of the user information the end-node is authorized to transmit and receive through the edge node packets in an authentication flow involving the end-node and wherein at least in part in response to the verification of the user information the end-node is authorized to transmit and receive through the edge node packets in data flows involving the end-node, and

wherein the edge node performs LAN media translations on the packets in the data flows.

46. An edge node for authorizing an end-node, the edge node comprising:

an interface for receiving user information from the end-node via a LAN link for verification,

wherein prior to verification of the user information the end-node is authorized to transmit and receive through the edge node packets in an authentication flow involving the end-node and wherein at least in part in response to verification of the user information the end-node is authorized to transmit and receive through the edge node packets in data flows involving the end-node, and

wherein the edge node switches the packets in the data flows based at least in part on MAC addresses.

47. An edge node for authorizing an end-node, the edge node comprising:

an interface for receiving user information from the end-node via a LAN link for verification,

wherein the end-node accesses the edge node via the interface and wherein at least in part in response to verification of the user information the interface transitions from an unauthenticated to an authenticated state, whereupon the edge node is authorized to transmit and receive packets in data flows involving the end-node and other nodes in the institutional LAN.

48. The edge node of claim 47, wherein the interface reverts to the unauthenticated state if a packet is not received from the end-node for a predetermined time period.

49. The edge node of claim 47, wherein the interface reverts to the unauthenticated state upon detecting that the end-node has become disconnected.

50. An edge node for authorizing an end-node, the edge node comprising:

an interface for receiving user information from an end-node via a LAN link for verification,

wherein the end-node accesses the edge node via a LAN interface and wherein at least in part in response to verification of the user information the interface transitions from an unauthenticated to an authenticated state, whereupon the edge node is authorized to transmit and receive packets in data flows involving the end-node, and

wherein the edge node performs LAN media translations on the packets in the data flows.

51. An edge node for authorizing an end-node, the edge node comprising:

an interface for receiving user information from the end-node via a LAN link for verification,

wherein the end-node accesses the edge node via the interface and wherein at least in part in response to verification of the user information the interface transitions from an unauthenticated to an authenticated state, whereupon the edge node is authorized to transmit and receive packets in data flows involving the end-node, and

wherein the edge node switches the packets in the data flows based at least in part on MAC addresses.

B1

52. An edge node for authorizing an end-node to an institutional LAN, the edge node comprising:

an interface for receiving user information from the end-node via a LAN link for verification,

wherein the edge node regulates packet flows from the end-node to an institutional LAN including verifying the user information.

53. An edge node for authorizing an end-node to an institutional LAN, the edge node comprising:

an interface for receiving user information from the end-node via a LAN link for verification,

wherein the edge node regulates packet flows from the end-node including verifying the user information and performing LAN media translations.

54. An edge node for authorizing an end-node to an institutional LAN, the edge node comprising:

an interface for receiving user information from the end-node via a LAN link for verification,

wherein the edge node regulates packet flows from the end-node including verifying the user information and performing LAN switching based at least in part on MAC addresses.

55. An authentication agent for representing an edge node in an authentication protocol exchange with an end-node for access to an institutional LAN, the agent comprising:

means for transmitting a request for user information via a LAN link to the end-node;

means for receiving user information from the end-node via a LAN link in response to the request;

means for transmitting the user information to an authentication server for verification;

means for receiving verification information from the authentication server at least in part in response to the user information; and

means for regulating access of the end-node to services of the institutional LAN available through the edge node in response to the verification information.

56. The authentication agent of claim 55, wherein the authentication agent is a software program.

57. The authentication agent of claim 55, wherein the authentication agent is resident on the edge node.

58. The authentication agent of claim 55, wherein the authentication agent further includes means for transmitting the verification information to the end-node.

64. (Amended) A user authentication system comprising:

an edge node;

an interface on the edge node for receiving an authentication information from an end-node via a LAN link for verification; and

an authentication server coupled to the edge node,

wherein the edge node forwards the authentication information to the authentication server and the authentication server verifies the authentication information and provides a notification to the edge node that the authentication information has been verified, whereupon the edge node is authorized to provide LAN switching functions for packets in data flows involving the end-node, wherein the LAN switching functions include performing LAN media translations on the packets.

B1

66. An authentication system for authorizing an end-node, the system comprising:

a LAN interface for receiving user information from the end-node via a LAN link;

an authentication agent for receiving the user information from the LAN interface via a switching link;

a backbone interface for receiving the user information from the authentication agent via the switching link; and

an authentication server for receiving the user information from the backbone interface for verification,

wherein prior to verification of the user information the LAN interface transmits on the switching link packets in an authentication flow involving the end-node and wherein at least in part in response to verification of the user information the LAN interface is authorized to transmit on the switching link packets in data flows involving the end-node.

71. A method for representing an edge node in an authentication protocol exchange with an end-node for access to an institutional LAN, the method comprising:

transmitting a request for user information via a LAN link to the end-node;

receiving user information from the end-node via the LAN link in response to the request;

transmitting the user information to an authentication server for verification;

receiving verification information from the authentication server at least in part in response to the user information; and

regulating access of the end-node to services of the institutional LAN available through the edge node in response to the verification information.

72. The method of claim 71 further comprising the step of transmitting the verification information to the end-node.

73. A user authentication system for an institutional LAN having an edge node, the system comprising:

an end-node; and

an interface on the end-node for transmitting user information via a LAN link to the edge node for verification,

wherein prior to verification of the user information the end-node is authorized to transmit and receive through the edge node packets in an authentication flow involving the end-node and wherein at least in part in response to the verification of the user information the end-node is authorized to transmit and receive through the edge node packets in data flows involving the end-node and other nodes in the institutional LAN.

74. A user authentication system for an institutional LAN having an edge node, the system comprising:

an end-node; and

an interface on the end-node for transmitting user information via a LAN link to the edge node;

wherein prior to verification of the user information the end-node is authorized to transmit and receive through the edge node packets in an authentication flow involving the end-node and wherein at least in part in response to verification of the user information the end-node is authorized to transmit and receive through the edge node packets in data flows involving the end-node, and

wherein the edge node performs LAN media translations on the packets in the data flows.

75. A user authentication system for an institutional LAN having an edge node, the system comprising:

an end-node; and

an interface on the end-node for transmitting user information via a LAN link to the edge node for verification,

wherein prior to verification of the user information the end-node is authorized to transmit and receive through the edge node packets in an authentication flow involving the end-node and wherein at least in part in response to verification of the user information the end-node is authorized to transmit and receive through the edge node packets in data flows involving the end-node, and

wherein the edge node switches the packets in the data flows based at least in part on MAC addresses.

76. A user authentication system for an institutional LAN having an edge node with a first interface, the system comprising:

an end-node; and

a second interface on the end-node for transmitting user information via a LAN link to the edge node for verification,

wherein the end-node accesses the edge node via the first interface and wherein at least in part in response to verification of the user information the first interface transitions from an unauthenticated to an authenticated state, whereupon the end-node is authorized to transmit and receive via the edge node packets in data flows involving the end-node.

77. The system of claim 76, wherein the first interface reverts to the unauthenticated state if a packet is not received from the end-node for a predetermined time period.

78. The system of claim 77, wherein the first interface reverts to the unauthenticated state upon detecting that the end-node has become disconnected.

79. A user authentication system for an institutional LAN having an edge node with a first interface, the system comprising:

an end-node; and

a second interface on the end-node for transmitting user information via a LAN link to the edge node for verification,

wherein the end-node accesses the edge node via the first interface and wherein at least in part in response to verification of the user information the first interface transitions from an unauthenticated to an authenticated state, whereupon the end-node is authorized to transmit and receive via the edge node packets in data flows involving the end-node, and

wherein the edge node performs LAN media translations on the packets in the data flows.

80. A user authentication system for an institutional LAN having an edge node with a first interface, the system comprising:

an end-node; and

a second interface on the end-node for transmitting user information via a LAN link to the edge node for verification,

wherein the end-node accesses the edge node via the first interface and wherein at least in part in response to verification of the user information the first interface transitions from an unauthenticated to an authenticated state, whereupon the end-node is authorized to transmit and receive via the edge node packets in data flows involving the end-node, and

wherein the edge node switches the packets in the data flows based at least in part on MAC addresses.

81. A user authentication system for an institutional LAN having an edge node, the system comprising:

an end-node having a user interface for receiving user information and a LAN interface for transmitting the user information via a LAN link to the edge node,

wherein the end-node is authorized to send and receive through the edge node packets in data flows involving the end-node only after verification of the user information.

82. A user authentication system for an institutional LAN having an edge node, the system comprising:

an end-node having a user interface for receiving user information and a LAN interface for transmitting the user information via a LAN link to the edge node,

wherein the edge node regulates packet flows from the end-node including subjecting the user information to verification and performing LAN media translations.

83. A user authentication system for an institutional LAN having an edge node, the system comprising:

an end-node having a user interface for receiving user information and a LAN interface for transmitting the user information via a LAN link to the edge node,

wherein the edge node regulates packet flows from the end-node including subjecting the user information to verification and performing LAN switching based at least in part on MAC addresses.

84. An authentication client for representing an end-node in an authentication protocol exchange with an edge node coupled to the end-node via a LAN link to obtain access for the end-node to services of an institutional LAN available through the edge node, the client comprising:

means for receiving a request for user information from the edge node; and

means for transmitting user information to the edge node in response to the request.

85. The authentication client of claim 84, wherein the authentication client is a software program.

86. The authentication client of claim 84, wherein the authentication client is resident on the end-node.

87. The authentication client of claim 84, further comprising means for receiving a request for second user information from the edge node in response to the user information.

88. The authentication client of claim 87, further comprising means for transmitting the second user information to the edge node in response to the request for second user information.

89. The authentication client of claim 88, further comprising means for receiving verification information from the edge device in response to the second user information.

90. The authentication client of claim 84, wherein the end-node is a personal computer.

91. The authentication client of claim 84, further comprising means for receiving verification information from the edge device in response to the user information.

92. A system for authenticating a user including an edge node and an authentication server coupled to the edge node, the system comprising:

an end-node having a user interface for receiving a authentication information and a LAN interface for transmitting the authentication information on a LAN link to the edge node,

wherein the edge node forwards the authentication information to the authentication server and the authentication server verifies the authentication information and provides a notification to the edge node that the authentication information has been verified, whereupon the end-node is authorized for access to services of a LAN infrastructure via the edge node.

93. A system for authenticating a user including an edge node and an authentication server coupled to the edge node, the system comprising:

an end-node having a user interface for receiving a authentication information and a LAN interface for transmitting the authentication information on a LAN link to the edge node,

wherein the edge node forwards the authentication information to the authentication server and the authentication server verifies the authentication information and provides a notification to the

edge node that the authentication information has been verified, whereupon the edge node is authorized to provide LAN switching functions for packet flows involving the end-node.

94. The system of claim 93, wherein the LAN switching functions include forwarding and filtering in function of MAC addresses.

95. The system of claim 93, wherein the LAN switching functions include LAN media translations.

96. A system for authenticating a user including an edge node and an authentication server coupled to the edge node, the system comprising:

an end-node having a user interface for receiving a authentication information and a LAN interface for transmitting the authentication information on a LAN link to the edge node,

wherein a message exchange between the edge node and the authentication server is conducted to verify the authentication information, whereupon the end-node is authorized for access to services of an institutional LAN via the edge node, and

wherein a security protocol is applied to secure the message exchange between the edge node and the authentication server.

97. A system for authenticating a user including an edge node and an authentication server coupled to the edge node, the system comprising:

an end-node having a user interface for managing interactions with the user in an authentication protocol exchange and a LAN interface for managing interactions on a LAN link with the edge node in the authentication protocol exchange,

wherein the edge node forwards information concerning the authentication protocol exchange to the authentication server in

response to which the authentication server generates and stores in a database tracking information concerning the authentication protocol exchange.

98. The system of claim 97, wherein the tracking information includes user information.

99. The system of claim 97, wherein the tracking information includes network location information.

100. The system of claim 97, wherein the tracking information includes time-of-day information.

B1

101. A method for representing an end-node in an authentication protocol exchange with an edge node coupled to the end-node via a LAN link to obtain access for the end-node to services of an institutional LAN available through the edge node, the method comprising:

receiving a request for user information from the edge node; and

transmitting user information to the edge node in response to the request.

102. The method of claim 101, further comprising the step of receiving first verification information from the edge node in response to the user information.

103. The method of claim 102, further comprising the step of receiving a request for second user information from the edge node in response to the first verification information.

104. The method of claim 103, further comprising the step of transmitting second user information to the edge node in response to the request for second user information.

105. The method of claim 104, further comprising the step of receiving second verification information from the edge device in response to the second user information.

106. An authentication system for authorizing an end-node to an institutional LAN, the system comprising:

an edge node having an interface for receiving a first response containing first user information and second response containing second user information from the end-node via a LAN link for verification, and

wherein prior to verification of the second user information the end-node is authorized to transmit and receive through the edge node packets in an authentication flow involving the end-node and wherein the end-node is authorized in response to the verification of the second user information to transmit and receive through the edge node packets in data flows involving the end-node and other nodes in the institutional LAN.

107. The system of claim 106 wherein the second user information is received after verification of the first user information.

108. (Amended) The system of claim 106, further comprising an authentication server coupled to the edge node wherein the edge node transmits the second user information to the authentication server, and the authentication server verifies the second user information.

109. A user authentication system for authorizing an end-node to an institutional LAN, the system comprising:

an edge node having an interface for receiving first user information and second user information from the end-node via a LAN link for verification,

wherein the edge node causes verification of the first user information, and upon verification of the first user information, the edge node receives and causes verification of the second user information, and

wherein in response to verification of the second user information the interface transitions from an unauthenticated to an authenticated state, whereupon the edge node is authorized to transmit and receive packets in data flows involving the end-node and other nodes in the institutional LAN.

B1

110. An edge node for authorizing an end-node to an institutional LAN, the edge node comprising:

an interface for receiving first user information and second user information from the end-node via a LAN link for verification,

wherein the edge node regulates packet flows from the end-node to an institutional LAN including causing verification of the first user information and second user information.

113. A method for authorizing an end-node to an institutional LAN having a plurality of nodes including an edge node, the method comprising:

transmitting from the end-node to the edge node via a LAN link first user information;

receiving a request for second user information upon verification of the first user information;

transmitting the second user information in response to the request;

obtaining, upon verification of the second user information, authorization to transmit and receive through the edge node packets in data flows involving the end-node and the other nodes in the institutional LAN.

114. (Amended) The method of claim 113, further comprising the step of performing LAN media translations within the edge node on packets transferred by the end-node through the edge node after the second verification.

115. (New) A system for authorizing a user on an end-node to a LAN infrastructure, the system comprising:

an edge node; and

an interface associated with the edge node for receiving user information from an end-node via a LAN link for verification; and

an authentication server coupled to the edge node,

wherein the edge node forwards the user information to the authentication server and the authentication server verifies the user information and provides a notification to the edge node that the user information has been verified, whereupon the user is authorized for access to services of a LAN infrastructure via the edge node.

116. (New) The system of claim 115, wherein the authentication server is a RADIUS server.

117. (New) An authentication system for authorizing an end-node, the system comprising:

an edge node;

an interface associated with the edge node for managing interactions on a LAN link with the end-node in an authentication protocol exchange; and

an authentication server coupled to the edge node;

wherein the edge node forwards user information concerning the authentication protocol exchange to the authentication server in response to which the authentication server generates and stores in a database tracking information concerning the authentication protocol exchange.

118. (New) The system of claim 117, wherein the tracking information includes user information.

119. (New) The system of claim 117, wherein the tracking information includes network location information.

B1

120. (new) The system of claim 117, wherein the tracking information includes time-of-day information.

121. (New) A method for authorizing an end-node to an institutional LAN having a plurality of nodes including an edge node, the method comprising:

enabling an authentication flow between the end-node and the edge node via a LAN link;

receiving first user information from the end-node;

performing a first verification attempt on the first user information;

depending upon a result of the first verification attempt, soliciting or not second user information from the end-node;

performing a second verification attempt on the second user information; and

depending upon a result of the second verification attempt, authorizing or not the end-node to transmit and receive through the edge node packets in data flows involving the end-node and the other nodes in the institutional LAN.

122. (New) A user authentication system comprising:

an edge node;

an interface on the edge node for receiving user information from an end-node via a LAN link for verification; and

an authentication server coupled to the edge node;

wherein the edge node forwards the user information to the authentication server and the authentication server verifies the user information and provides a notification to the edge node that the user information has been verified, whereupon the edge node is authorized to provide LAN switching for packets in data flows involving the end-node.

123. (New) A user authentication system comprising:

an edge node;

an interface on the edge node for receiving user information from an end-node via a LAN link for verification; and

an authentication server coupled to the edge node via a secure connection;

wherein the edge node forwards the user information to the authentication server via the secure connection and the authentication server verifies the user information and provides a notification to the edge node via the secure connection that the user information has been verified, whereupon the edge node authorizes transmission on the edge node of packets in data flows involving the end-node.

124. (New) A user authentication system comprising:

an edge node;

an interface on the edge node for receiving user information from an end-node via a LAN link for verification; and

an authentication server coupled to the edge node;

wherein the edge node forwards the user information to the authentication server and the authentication server verifies the

user information and provides a notification to the edge node that the user information has been verified, whereupon the edge node authorizes communication within a VLAN of packets in data flows involving the end-node.

125. (New) The system of claim 124, wherein the notification identifies the VLAN.

126. (New) A user authentication system for a communication network, comprising:

an end-node;

an edge node communicating with the end-node over a LAN link; and

an authentication server coupled to the edge node;

wherein an authentication session is conducted in which the edge node attempts to collect from the end-node and verify on the authentication server user information, and wherein the edge node terminates the authentication session upon completing a plurality of failed attempts.

127. (New) The system of claim 126, wherein the authentication server is a RADIUS server.

REMARKS

By this amendment, Applicants voluntarily cancel certain claims (claims 59-63, 65, 67-70, 111 and 112) and add and amend certain others (claims 115-127 added; claims 64, 108 and 114 amended) to more clearly recite the subject matter of the invention. Claims 44-58, 64, 66, 71-110, and 113-127 are presently pending.